CNS-105-2 Critique #7 : An Analysis of China's "Great Cannon"

B03901027　徐彥旻

B. Marczak, N. Weaver, J. Dalek, R. Ensafi, D. Fifield, S. Mckune,A. Rey, J. Scott-Railton, R. Deibert, and V. Paxson, "An Analysis of China's 'Great Cannon,'" in USENIX Workshop on Free and Open Communications on the Internet (FOCI 15), 2015.

Summary

中國的網路長城其實不是防火牆，而是中間人攻擊，網路長城會將每個連結的封包做整體性的分析以提高審查的正確率，也有機制(可能是用電腦叢集)來平衡每個實體連結的負擔。

而 GC 則是只分析牽涉其鎖定的位置的網路交通，對各別的封包做分析而不是對整個連結的封包做整體性的分析，此外也有將之前審查過認為不需要再審查的連結快取起來，將低了計算的負擔，能夠讓整個系統跟得上非常大量的網路交通。當境外的使用者向百度的主機要求特定的 Javascript 檔，GC 觀察到之後，會機率性的阻斷這個要求，並回傳給使用者惡意的 script。

雖然政府否認，但是由於 GC 跟 GFW 在不同的 ISP 上都有同樣的位置， TTL side-channel 的類型也一模一樣，因此 GC 應該是由政府在運轉的。而政府拿百度來當作目標，可能代表比起國內重要網路公司的聲譽與經濟上的利益，更重視國家的言論審查與國內的穩定。

在未來可能會出現的改進當中，比較簡單的改進除了是將連到特定網站的使用者設為目標之外，從特定 IP 連過來的使用者也可以納入攻擊的範圍。更進一步， GC 還可以藉由 fully stateful MITM proxy 的實作來進行降級攻擊。

Strength(s)

- 經由實驗與紀錄分析，確認攻擊的存在、來源與程度。
- 分析攻擊者採用這個攻擊的利弊，以及攻擊者可能是誰。
- 提出未來這樣的攻擊可能會有的進展。
- 提出防禦的對策：應盡快將所有的 HTTP 換為 HTTPS。

Weakness(es)

- 實驗的結果可以用圖表呈現，會比較好懂。

Reflection

我學到了結合中間人攻擊與分散式阻斷攻擊結合的例子，並且知道了可能的防禦方式。至於在風險模型與假設的部分，大致上沒有什麼問題，因為這個研究是對現存的攻擊進行分析。

然而，為何中國會架設如此明顯的攻擊則是這篇論文新提出來的疑惑，也沒有初步的解答。這部分的分析可能要考慮到這個系統裡頭的 human element，甚至還會有政治經濟的分析，而不太能夠藉由論文裡頭的實驗得知。

其他可能的防禦：不要連百度。不要連中國網站。